EXHIBIT 4

PBS NEWSHOUR

Hacking researchers kill a car engine on the highway to send a message to automakers

July 22, 2015 at 6:30 PM EDT

Driving on a highway in St. Louis, WIRED writer Andy Greenberg allowed himself to get car-hacked. Two researchers were able to remotely blast the stereo on his SUV, turn on the windshield wipers and kill the engine. Today, vehicles function almost like smartphones on wheels, but that convenience allows hackers to engage in wireless sabotage. Greenberg joins Hari Sreenivasan to discuss the dangers.

TRANSCRIPT

GWEN IFILL: Now a cautionary tale of a different kind of computer hacking that you will want to see.

Hari Sreenivasan has the story from our New York studios.

ANDY GREENBERG, WIRED: It's not fun to have your two-ton SUV's brakes hacked just as you're parking in front of a ditch.

HARI SREENIVASAN: Writer Andy Greenberg found that out the hard way. For a story on Wired.com, he decided to be a willing victim of car hacking by two researchers, Charlie Miller and Chris Valasek. The two-and-a-half-ton guinea pig? A 2014 Jeep Cherokee that Greenberg drove on a Saint Louis highway.

CHARLIE MILLER, Security Engineer, Twitter: Remember, Andy, no matter what happens, don't panic.

HARI SREENIVASAN: That's easier said than done. Without warning, and from miles away, they

blasted the air vents, and started blaring the music.

ANDY GREENBERG: I can't turn it down.

HARI SREENIVASAN: After turning on the windshield wipers and wiper fluid, they killed the engine, forcing him to bring the car to a halt on the highway, as cars and semis sped by.

ANDY GREENBERG: All right, I'm going to pull over, because I have PTSD.

HARI SREENIVASAN: The hack is possible through an Internet-connected system in the car called Uconnect that controls the entertainment and navigation, and enables communication through phone calls and Wi-Fi.

Below a certain speed, hackers can even control the jeep's steering, as long as it's in reverse. They can adjust the locks, and disable the brakes. Many automakers now produce vehicles that function like smartphones on wheels, but that convenience also allows hackers to now engage in wireless carjacking.

Miller and Valasek have been researching car hacking for years, and found the Jeep Cherokee to be the most hackable model.

CHARLIE MILLER: These cars had units exposed to a particular service that probably they didn't want to. It lets you do things like query it for information like the GPS or the VIN or some other things, but it also lets you just run commands.

HARI SREENIVASAN: Miller and Valasek alerted Chrysler, sharing their research for months. The company, however, is wary of this disclosure.

CHRIS VALASEK, Director of Vehicle Security Research IOActive: We want to release this information because more people like us need to be focused on this problem.

HARI SREENIVASAN: Just yesterday, Senators Ed Markey and Richard Blumenthal introduced legislation that requires cars sold in the U.S. to meet standards of protection against digital attacks.

For more about the vulnerabilities and the concerns around all this, Andy Greenberg, senior writer for "Wired" magazine, joins me now.

So, why did you do the hack?

ANDY GREENBERG: Well, this was all actually the work of Charlie Miller and Chris Valasek, these two researchers.

They have been trying to do this for three years to actually gain Internet wireless access to a vehicle remotely. And they finally succeeded. And this is the first time not only that they have demonstrated that, which they did to me on the highway, but also that they have named the automaker, they have detailed some of the — how they did it.

And they are going to talk about this at a conference next month. And they're finally going to actually release some of the code itself, so that — not enough that it could be easily replicated, but enough that other researchers can see what they have done, can test it out. This is like how good science is done.

And I think all of it is meant to send a message to pressure the car industry to solve these problems, to take security vulnerabilities seriously.

HARI SREENIVASAN: How easy or difficult is it? Should we be concerned that there's, what, 400,000 cars with this kind of software inside it?

ANDY GREENBERG: Everybody who has this one computer, Uconnect, in their Chrysler dashboard needs to download this patch that Chrysler actually released very quietly last week.

And they can download it to their computer, put it on a USB drive and just update the software and protect themselves from this serious attack. But the question is whether somebody else could create a new hacking technique that would affect Chrysler vehicles or others. And that's very possible, but it's not easy.

Both of these guys are brilliant hackers. One of them is a former NSA analyst. I wouldn't expect

some kid in their basement to come up with a new technique, but with what is already out there, anybody can do what Charlie Miller and Chris Valasek have done to at least mess with the dashboard functions. And that's mischief enough.

HARI SREENIVASAN: So, let me get this right. My phone can get an update automatically from Google or from Apple, but Chrysler is not automatically updating the cars. Can you take it into your dealer and have it done that way?

ANDY GREENBERG: Right. For the Chrysler vehicles that need this patch, you have to do it yourself with a USB drive or take it to the dealership.

Some carmakers already do what they call over-the-air updates, where they don't automatically update, but you can do it from the computer itself in the car. And, in fact, every automaker practically is moving towards over-the-air updates. They know that this is a fix that needs to happen.

HARI SREENIVASAN: One of the things that every automaker is also moving toward is having greater amounts of technology in cars, right, basically, these smartphones on wheels.

And when we think of the Internet of things, how everything's getting so connected, does that just mean that everything is also so much more hackable?

ANDY GREENBERG: When I talk to security experts about the whole industry, they say that, yes, the industry is trying to solve this problem, but things are getting worse faster than they're getting better, and that's because the auto industry just wants to add these features.

They're competing to have more interconnected features, navigation, and safety and entertainment and that those things also provide a nice monthly revenue stream for the cellular service. So every one of those features is also a potentially hackable bug, too.

HARI SREENIVASAN: There's also the piece of current legislation that was proposed yesterday by a couple of senators, but when is there a scenario where the law and technology are on the same playing field? Sometimes, it seems like the law is 10 years behind catching up to

technology to try to legislate it and regulate it.

ANDY GREENBERG: I think that there are legal standards for the safety of automobiles. They have to have seat belts, they have to have air bags, you know, so this is kind of the modern equivalent.

It will be, of course, very difficult to legislate something this complex. This isn't just a safety issue. It's kind of a cat-and-mouse game with a whole world of hackers, and it has to be a dynamic kind of solution to a very dynamic problem.

So, you know, it's not entirely clear that legislation can fix this, but what is clear is that the auto industry needs to wake up somehow. Whether that is through consumer pressure, per their own self-regulation or through Congress taking action, something needs to happen.

HARI SREENIVASAN: Hacking seems to follow every sort of online leap forward. Right? Bank accounts have been hacked, credit card companies and so forth, the transactions that we have from multiple vendors. Having your car hacked, when you were driving that car, what was going through your head when you basically lost control step by step?

ANDY GREENBERG: Well, it's incredibly unnerving.

You kind of — if you have driven for some number of years and you have come to assume that the pedal does something and the steering wheel does something, and to realize that it's just kind of a fallible machine that can even be controlled by someone else or kind of what feels just like a virtual invisible force somewhere far away, it definitely produces a unique kind of anxiety.

HARI SREENIVASAN: Was it the smartest idea to do it on a freeway in Saint Louis?

ANDY GREENBERG: In retrospect, maybe not.

But I wasn't — I didn't actually know what these guys were going to do. They said — they just told me to drive onto the highway. And then at first, they were just messing with the radio and the windshield wipers. When they cut the transmission, I was shocked myself.

And I think probably all of us — they didn't know, for instance, that there wasn't going to be a shoulder at the point when they did it to the highway. So, in — maybe all of us would have chosen to do it on a closed course if we would have known how it would have gone.

But in the end, I think it was important to show how scary it can be. Nobody was hurt. And in the end, we have this example instead of just how dangerous this kind of vulnerability is. And I think it sends an important message.

HARI SREENIVASAN: Andy Greenberg of Wired, thanks so much for joining us.

ANDY GREENBERG: Thank you.